# UNITED STATES DISTRICT COURT

for the

Western District of North Carolina

| | | |
|---|---|---|
| In the Matter of the Search of<br>*(Briefly describe the property to be searched or identify the person by name and address)*<br>The premises, outbuilding, vehicles, and curtilage located at 531 Pet Road, Murphy, North Carolina 28906 | ) | Case No. 1:20-mj-33 |

## APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*
See Attachment A to the accompanying Affidavit.

located in the Westen District of North Carolina, there is now concealed *(identify the person or describe the property to be seized)*:
See Attachment B to the accompanying Affidavit.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

| *Code Section* | *Offense Description* |
|---|---|
| 18 U.S.C. § 2252A(a)(2)(A) | Receipt of Child Pornography |
| 18 U.S.C. § 2252A(a)(5)(B) | Possession of Child Pornography |

The application is based on these facts:

See accompanying Affidavit.

- ☒ Continued on the attached sheet.
- ☐ Delayed notice 30 days (give exact ending date if more than 30 _____ ) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

/s/ Roger L. Williams
*Applicant's signature*

Roger L. Williams, HSI Task Force Officer
*Printed name and title*

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P 4.1 by (telephone)

Signed: May 27, 2020

Date: 5/27/2020

W. Carleton Metcalf
United States Magistrate Judge

City and state: Asheville, North Carolina — The Hon. W. Carleton Metcalf, U.S. Magistrate Judge
*Printed name and title*

# AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, R. L. Williams, a Task Force Officer with Homeland Security Investigations, being duly sworn, depose and state as follows:

## INTRODUCTION

1. I am investigating offenses related to child sexual exploitation. This Affidavit is submitted in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises located at 531 Pet Lane, Murphy, North Carolina 28906 (the "SUBJECT PREMISES"), more specifically described in Attachment A, for contraband and evidence, fruits, and instrumentalities of violations of Title 18 U.S.C. §§ 2252A(a)(2)(A) and 2252A(a)(5)(B), which items are more specifically described in Attachment B.

2. The statements in this Affidavit are based in part on information provided by other law enforcement officers and on my investigation of this matter. Since this Affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that contraband and evidence, fruits, and instrumentalities of violations of Title 18 U.S.C. §§

2252A(a)(2)(A) and 2252A(a)(5)(B) are presently located at the SUBJECT PREMISES.

## AFFIANT BACKGROUND

3. I am employed as a Detective with the Cherokee County Sheriff's Office, Cherokee County North Carolina. I am assigned as a Task Force Officer ("TFO") with Homeland Security Investigations ("HSI"), a division of Immigration and Customs Enforcement, Hendersonville North Carolina, assigned to the Special Agent in Charge ("SAC") Charlotte North Carolina. I have been employed as a law enforcement officer for over 38 years. I have been assigned as a full time TFO with the Hendersonville Resident Agent in Charge ("RAC") by HSI since April 2018. As a TFO with HSI, I have investigated federal criminal violations related to high technology or cybercrime, child exploitation, and child pornography. I have gained experience through training at the Federal Law Enforcement Training Center ("F.L.E.T.C.") and everyday work relating to conducting these types of investigations. I have received training in the area of child pornography and child exploitation, and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media. I am a member of the North Carolina Internet Crimes Against Children ("North Carolina ICAC") Taskforce and am currently

assigned to conduct child exploitation investigations for the RAC Hendersonville, North Carolina. Moreover, I am a federal task force officer who is engaged in enforcing the criminal laws, including 18 U.S.C. §§ 2252 and 2252A, and I am authorized by law to request a search warrant.

## STATUTORY AUTHORITY

4. As noted above, this investigation concerns alleged violations of the following:

a. 18 U.S.C. § 2252A(a)(2)(A) prohibits a person from knowingly receiving or distributing child pornography, as defined in 18 U.S.C. § 2256(8), using any means and facility of interstate and foreign commerce, that has been mailed, or that has been shipped and transported in and affecting interstate and foreign commerce by any means, including by computer. Attempts and conspiracies are also violations of this statute. 18 U.S.C. § 2252A(b)(1).

b. 18 U.S.C. § 2252A(a)(5)(B) prohibits a person from knowingly possessing or knowingly accessing with intent to view any material that contains an image of child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, or

that was produced using materials that have been mailed or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer. Attempts and conspiracies are also violations of this statute. 18 U.S.C. § 2252A(b)(2).

**DEFINITIONS**

5. The following definitions apply to this Affidavit and Attachment B:

a. "Chat," as used herein, refers to any kind of text communication over the Internet that is transmitted in real-time from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

b. "Child erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily obscene or do not necessarily depict minors engaging in sexually explicit conduct.

c. "Child pornography," as defined in 18 U.S.C. § 2256(8), is any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or

produced by electronic, mechanical or other means, of sexually explicit conduct, where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

d. "Computer," as used herein, refers to "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device" and includes smartphones, other mobile phones, and other mobile devices. *See* 18 U.S.C. § 1030(e)(1).

e. "Computer hardware," as used herein, consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including central processing units, internal and peripheral storage devices such as fixed disks, external hard drives,

"thumb," "jump," or "flash" drives, which are small devices that are plugged into a port on the computer, and other memory storage devices); peripheral input/output devices (including keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including physical keys and locks).

f. "Computer passwords and data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates what might be termed a digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

g. "Geolocated," as used herein, refers to the identification of the geographical location of (a person or device) by means of digital information processed via the Internet.

h. "Hashtag," as used herein, refers to a word or phrase preceded by a hash or pound sign (#), which is used to identify messages or groups on a specific topic.

i. A "hash value" is a unique multi-character number that is associated with a computer file. Some computer scientists compare a hash value to an electronic fingerprint in that each file has a unique hash value. Any identical copy of the file will have exactly the same hash value as the original, but any alteration of the file, including even a change of one or two pixels, would result in a different hash value. Hash values represent large amounts of data as much smaller numeric values, so they are used with digital signatures.

j. "ICAC Data System" ("IDS") is a web based system whereby Cyber Tips issued by the National Center for Missing and Exploited Children are distributed to ICAC Investigators. The West Virginia State Police designed and has maintained IDS since 2014. IDS allows for the transfer of cases to investigators, affiliates, and other task forces without delay. This system is intended to facilitate data deconfliction among

ICAC task force agencies. IDS can also function as a case management system for smaller agencies that do not have a system in place to provide this functionality.

k. "Internet Service Providers" ("ISPs"), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, email, remote storage, and co-location of computers and other communications equipment.

l. An "Internet Protocol address" or "IP address," as used herein, refers to a unique numeric or alphanumeric string used by a computer or other digital device to access the Internet. Every computer or device accessing the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer or device may be directed properly from its source to its destination. Most Internet Service Providers ("ISPs") control a range of IP addresses. IP addresses can be "dynamic," meaning that the ISP assigns a different unique number to a computer or device every time it accesses the Internet. IP addresses might also be "static," if an ISP assigns a user's computer a particular IP address that is used each time the computer accesses the Internet. ISPs

typically maintain logs of the subscribers to whom IP addresses are assigned on particular dates and times.

m. The "Internet" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

n. "Minor," as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

o. "Mobile application" or "chat application," as used herein, are small, specialized programs downloaded onto mobile devices, computers and other digital devices that enable users to perform a variety of functions, including engaging in online chat and sending or receiving images and videos.

p. "Records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

q. "Remote computing service", as defined in 18 U.S.C. § 2711(2), is the provision to the public of computer storage or processing services by means of an electronic communications system.

r. "Sexually explicit conduct," as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the anus, genitals, or pubic area of any person.

s. A "storage medium" is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, "thumb," "jump," or "flash" drives, CD-ROMs, and other magnetic or optical media.

t. "Tumblr" as used herein, is an American microblogging and social networking website founded in 2007. The service allows users to post multimedia and other content to a short-form blog. Users can follow other users' blogs. Bloggers can also make their blogs private. For bloggers many of the website's features are accessed from a "dashboard" interface.

u. "Visual depiction," as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

v. **"**Wi-Fi" is a wireless networking technology that allows computers and other devices to communicate over a wireless signal.

## BACKGROUND ON KIK AND KIK REPORTS

6. The following information has been provided to me by other law enforcement officers and also comes from online research that I have conducted as well as my training and experience. Kik Messenger, commonly called Kik, is a freeware instant messaging mobile app originally from the Canadian company Kik Interactive, available free of charge on iOS and Android operating systems. The Kik Messenger application is now owned and operated by MediaLab, a California-based holding company. Kik is a social networking application which permits a user to trade and disseminate various forms of digital media, while utilizing a wireless telephone. Kik advertises itself as "the first smartphone messenger with a built-in browser." Kik was founded in 2009 and according to their website, which I have viewed, was designed to "shift the center of computing from the PC to the phone." Kik is a free service easily

downloaded as an application from the Internet. Kik Messenger is a feature within Kik that allows its users to communicate to selected friends as well as browse and share any web site content with those whom the user selects, while still on the Kik platform. Unlike other messaging apps, Kik usernames - not phone numbers - are the basis for Kik user accounts. In addition, Kik features include more than instant messaging. Kik users can exchange images, videos, sketches, stickers and even web page content by posting such content privately with individual users (with whom the user selects) or publicly (on the Kik platform) with multiple individuals who belong to "Groups." Groups are formed when like-minded individuals join collectively online in an online forum, created oftentimes by a Kik user designated as the Kik "Administrator" of the group. Groups can hold up to 50 Kik usernames. Groups are created to host/discuss topics such as modern popular culture themed ideas as well as illicit/illegal themed ideas. Based on my training and experience, I know that Kik is often used for illegal activity, including the receipt, transportation and/or distribution of child pornography, because of the high degree of anonymity that is afforded to users during the use of the Kik application.

7. Kik is located in California, USA, and as such is governed by United States law. According to information contained in the "Kik Interactive, Inc. Child Sexual Abuse and Illegal Material Report and Glossary" (hereinafter

Kik Glossary), Kik is typically alerted to suspected child pornography on Kik based on digital hash value matches to previously identified child pornography or through reports from other Kik users or third party moderators.

8. According to the Kik Glossary, Kik enables users to report other users who have abused or harassed them within the application, using an in-application reporting feature. When a Kik user reports another user, they have the option to include their full conversation history, including text, and any images or videos sent between them. Kik refers to this type of report as an "Abuse Report."

9. According to the Kik Glossary, Kik uses PhotoDNA to automatically scan user-uploaded files in order to flag content that may depict suspected child pornography and prevent such images from continuing to circulate through their application. When PhotoDNA detects a suspected child pornography file, it creates a Report and sends it to the Kik Law Enforcement team. Kik refers to this type of report as a "PhotoDNA Report."

10. According to information provided by a Kik Law Enforcement Response Team Lead, all suspected child pornography images and videos reported via a PhotoDNA Report or an Abuse Report, as well as any related user communications, are visually reviewed by a member of the Kik Law Enforcement Response team before a report is forwarded to law enforcement

authorities. Kik trains employees comprising its Law Enforcement Response team on the legal obligation to report apparent child pornography. Kik voluntarily makes reports to law enforcement in accordance with that training. After Kik discovers suspected child pornography, Kik removes the content from its communications system and closes the user's account.

## PROBABLE CAUSE

11. On May 5, 2020, I received CyberTipline Report 65017754 reporting the suspected trading of child pornography by Kik user "childpussy1." The report concerned IP address 50.111.94.30 and listed 29 images and one video of child pornography that had been sent or received by the suspect user. The report revealed that, on February 10, 2020 at 06:30:55 UTC, "childpussy1" used IP address 50.111.94.30 to upload child pornography images and a child pornography video to Kik's servers.[1] More specifically, the report indicated that these files were "sent or received from this user to another user via private chat message." Information in CyberTipline Report 65017754 indicated that Kik was alerted to the image on February 27, 2020, at 17:07:34

[1] Coordinated Universal Time (or UTC) is the primary time standard by which the world regulates clocks and time. It is within about 1 second of mean solar time at 0° longitude, and is not adjusted for daylight saving time. It is effectively a successor to Greenwich Mean Time (GMT). Eastern Standard Time is equivalent to UTC minus 5 hours. Eastern Daylight Time is equivalent to UTC minus 4 hours. Thus, in this case 06:30:55 UTC converts to 1:30:55 AM EST.

UTC. The report indicated that Kik then reviewed the images and made a report to NCMEC who forwarded the report and the suspect images via the ICAC Data System (IDS).

12. I have reviewed the images and video reported by KIK to NCMEC and provide the following as a representative sample of the images/video uploaded by Kik user "childpussy1":

> File 1f04eff5-8c01-419d-b196-a7fb5e41c43b: This is a digital image of a prepubescent female laying on her back wearing a green top with her legs spread lewdly and lasciviously displaying her vagina and anus. This file was uploaded by "childpussy1" utilizing the IP address 50.111.94.30 on February 10, 2020 at 05:52:59 UTC.
>
> File e50540ad-edcd-4369-abf7-536fdef122d2: This is a digital image of a prepubescent female on her knees looking back over her shoulder with her panties pulled being held down by an adult's hand. There is a lewd and lascivious display of her vagina and anus. This file was uploaded by "childpussy1" utilizing the IP address 50.111.94.30 on February 10, 2020 at 05:57:33 UTC.
>
> File 847904cc-fe32-42f1-8eb6-26ac22c47e8e: This is a digital video file. It is approximately 1 minute and 11 seconds in length. It depicts a prepubescent nude female sitting on an adult male's lap who is also nude. They are sitting on a couch. The adult male is rubbing the vaginal area of the prepubescent female while his penis appears to be inserted into her vagina or anus. The nude prepubescent female gets up off the lap of the nude adult and moves to a position on the couch where she is on her hands and knees and the adult male positions himself behind her and inserts his penis into her anus. This file was uploaded by "childpussy1" utilizing the IP address 50.111.94.30 on February 10, 2020 at 07:09:53 UTC.

13. Provided along with CyberTipline Report 65017754 is a Kik subscriber record for user "childpussy1." This subscriber record reveals a "registration timestamp" for user "childpussy1" of February 7, 2020, at 21:53:29 UTC. The user provided his first name as "o" and his last name as "k." The Kik records list the email for user "childpussy1" as othat1019@gmail.com and state that the email address is "unconfirmed."[2] The user's device is identified as a Samsung Android (model number: SM-S327VL). The subscriber records also indicate that the user "childpussy1" accessed the Kik account 137 times during the period of February 7, 2020 21:53:33 UTC and February 10, 2020 07:35:53 UTC using IP address 50.111.94.30.

**Identification of a Residence at 531 Pet Lane, Murphy, Cherokee County, North Carolina as the Suspect's Residence**

14. Also provided with the information from the CyberTipline Report 65017754 was an administrative subpoena issued on April 5, 2020, by the North Carolina State Bureau of Investigation, requesting information pertaining to IP address 50.111.94.30 on February 10, 2020 at 05:59:54 GMT.[3]

[2] "Unconfirmed" means either that the email address is either invalid, or the user received a confirmation email from Kik but did not click on the link to confirm.
[3] "GMT" refers to Greenwich Mean Time. GMT and UTC times are equivalent to one another at all times relevant to this affidavit.

The administrative subpoena was directed to Frontier Communications, an internet service provider.

15. On April 22, 2020, Frontier Communications replied with the following information for the account subscriber information associated with IP address 50.111.94.30:

| | |
|---|---|
| Subscriber Name: | Earl & Jill Ruoss |
| Subscriber Address: | 531 Pet Lane Rd, Murphy NC 28906 |
| Phone Number: | 828-835-9189 |

The Frontier Communications records indicate that IP address 50.111.94.30 was assigned to the account of Earl & Jill Ruoss from at least February 7, 2020 at 20:51:14 UTC, through February 12, 2020 at 04:21:41 UTC. This time period covers the 137 connections reported by Kik concerning user "childpussy1" described in paragraph 13.

16. I checked the North Carolina Department of Motor Vehicle driver's license database and found a record that a Jill Ruoss has an active driver's license and that she reported her address as 531 Pet Lane Road, Murphy North Carolina. Her driver's license was renewed under this address on September 11, 2019.

17. I made a check of Cherokee County 911 Database records and located information that 531 Pet Lane Road, Murphy North Carolina is reported to be occupied by Earl Ruoss.

18. Despite the fact that the internet service registered to Jill and Earl Ruoss is tied to the trading of child pornography by Kik user "childpussy1," I do not believe that either Jill or Earl Ruoss are responsible for this activity. As I will describe in the paragraphs that follow, I believe Kik user "childpussy1" is an individual named **BRYCE HONEA** who is a tenant of Jill and Earl Ruoss and who on prior occasions regularly connected to their internet service and used it to download or access child pornography.

19. Since July 2018, I have been conducting several investigations involving reports of individual(s) that is/are sharing child pornographic images via the internet who were identified as residing in Cherokee County North Carolina. Several of these investigations led to one individual who I learned was actively and regularly downloading child pornography. In the paragraphs that follow, I will describe the various investigative steps that led me to identify **BRYCE HONEA** as a prolific trader and collector of child pornography. During these investigations, information provided by CyberTip Reports and legal processes that accompanied the CyberTip Reports identified two residences associated with **HONEA**: 2499 Ebenezer Road, Murphy North Carolina and 531 Pet Lane Road, Murphy North Carolina.

20. Specifically, on July 25, 2018, I was conducting an investigation of then unknown individuals who were offering to share child pornography over

the internet. During that investigation, I was able to identify a device using IP address 50.111.103.234 that was sharing child pornography. At that time, I was able to download 595 child pornographic files from the device connected to IP address 50.111.103.234.

21. I viewed the 595 files that had been shared via the internet on July 25, 2018. The follow are a representative of the nature and type of files that were shared on that date:

> ism-016-041.jpg: This image depicts a female child approximately 8-10 years of age who is seen completely naked. The girl has a ponytail which has a floral and multicolored tie in it. The girl is seated on a large rock near a body of water and is spreading her legs and exposing her vagina and breasts to the camera. A logo that says "LS island" can be seen in the upper right corner of the image.
>
> ism-016-051.jpg: This image file depicts a prepubescent female approximately 8 years old with brown hair pulled in a ponytail. She is wearing only a green ankle bracelet and is in a rocky area near a body of water. The girl is leaning back on her hands and feet with her legs spread as to clearly display her breast and genital area in a lewd and lascivious manner.
>
> ism-016-077.jpg: This image file depicts a naked prepubescent female sitting on a dirt mound in an outdoor setting. The young female is wearing a multi-colored sash around her waist and is looking directly at the camera. The young female has her legs spread wide apart exposing the inside area of her vagina in a lewd and lascivious manner and her breast area is also exposed. Up in the upper left corner of the image is the “LS island” logo.

21. On August 8, 2018, I requested that HSI generate a legal summons to provide subscriber information for IP address 50.111.103.234 at the time of

the downloads. The legal summons was directed to Frontier Communications of America, Inc. Frontier Communications of America, Inc. answered the legal summons indicating that IP address 50.111.103.234 was in fact registered to Frontier Communications of America, Inc. Further, the information provided in Frontier Communications of America, Inc.'s, response indicated that IP address 50.111.103.234 was assigned to the account of Earl and Jill Ruoss at 531 Pet Lane Road, Murphy, North Carolina 28906. The information provided by Frontier Communications of America, Inc. also provided that the IP address had been assigned from July 24, 2018 at 18:42:57 UTC to July 26, 2018 at 01:30:53 UTC. This time period covers the entire period of time in which I downloaded the previously described 595 child pornographic images.

22. On February 7, 2019, I executed a federal search warrant at 2499 Ebenezer Road, Murphy North Carolina. The search was based on information contained in a December 31, 2018, CyberTip Report 43674691 indicating that an individual had accessed the internet and shared 14 images of child pornography from a device located at the residence.

23. Included in CyberTip Report 43674691 was information that IP address 2001:5b0:46d7:d5e8:1576:5cf8:56a1:22ae[4] was associated with a

[4] This IP address appears in a different format than ones previously described because it is in what is known as Internet Protocol Version 6 or "IPv6" which is the most recent version of IP protocols.

Tumblr account that was used to transmit the 13 images and a video file of child pornography. Additionally the report provided that an email address of bhonea404@gmail.com had been used to establish the Tumblr.com account.

24. Included with the information in CyberTip Report 43674691 were 13 images and a video file that had been reported by Tumblr to NCMEC. I reviewed the files and provide the following as representative of the images and the video file:

180540835306_0_npf_video: is a video file approximately one minute and 30 seconds in length. It depicts a prepubescent female who is nude laying on her back and an adult male who is engaged in vaginal intercourse with the female.

178747724486_1_inline_image: is a digital image of two nude prepubescent females engaged in oral sex.

178747724486_3_inline_image: is a digital image of a minor making a lewd and lascivious display of genitalia.

25. Provided with CyberTip Report 43674691 was legal process issued by the North Carolina State Bureau of Investigation requesting subscriber information pertaining to IP address 2001:5b0:46d7:d5e8:1576:5cf8:56a1:22ae which was identified as belonging to Hughes.net. Subscriber information provided from Hughes.net was that the account associated with IP

2001:5b0:46d7:d5e8:1576:5cf8:56a1:22ae was leased to the Hughes.net account of Melinda "Beaber" [a suspected typo, believed to actually be "Beaver"] at 2499 Ebenezer Road, Murphy North Carolina. In a check of public records information I was able to determine that Melinda Beaver is **HONEA**'s mother.

26. During the search of the residence at 2499 Ebenezer Road, Murphy North Carolina, resident Melinda Beaver, stated that her son **BRYCE HONEA** had stayed at the residence a few months prior and had used the internet while staying there. Melinda Beaver further stated that **HONEA** had been staying there during the holidays, but had since returned to his home residence at 531 Pet Lane Road, Murphy North Carolina, which Melinda Beaver indicated was a short distance away.

27. Investigators with the Cherokee County Sheriff's Office went to 531 Pet Lane Road, Murphy North Carolina and were able to locate **HONEA**, who agreed to accompany the investigators back to 2499 Ebenezer Road, Murphy, North Carolina.

28. I interviewed **HONEA** while the search of the 2499 Ebenezer Road, Murphy North Carolina residence was being conducted. **HONEA** provided information that he had lived on "Joe Brown Highway" for several years but that he had moved away and was now living at 531 Pet Lane Road,

Murphy, North Carolina. **HONEA** told me that he leased a house at 531 Pet Lane Road from Jill Ruoss, who resides in an adjacent but separate residence to him which also uses the 531 Pet Lane Road address. **HONEA** said that Jill Ruoss has given him permission to use her Wi-Fi to access the internet. **HONEA** provided information that the internet account that he was accessing was with Frontier Communications. **HONEA** stated that during the start of the winter months of 2018, that he had stayed at the residence at 2499 Ebenezer Road, Murphy, North Carolina with his mother for a short period of time but had since returned to the 531 Pet Lane Road residence with his wife and two-year-old child.

29. During the interview, **HONEA** admitted that he has shared images of child pornography via the internet. He said that he would share images of child pornography in order to get additional images of child pornography. **HONEA** told me that he had previously shared child pornography while he was at the Joe Brown Highway residence, the 531 Pet Lane Road residence, and the 2499 Ebenezer Road residence. **HONEA** stated that he had used various social media applications such as Tumblr, Kik, Chatstep, Mega, and MeWe and he had used file sharing applications such as UTorrent to locate and obtain child pornography. **HONEA** stated that he would search message boards to find particular types of child pornography

images and gave an example of a series titled "LS" which he stated depicted young females who were semi-nude or nude and who displayed their genitalia. **HONEA** stated that after he viewed the images on his screen, he would then download the images to his computer.

30. During the interview, **HONEA** had in his possession a Samsung Galaxy S-6 which he stated he had used for the last three years. **HONEA** admitted that he had used the Samsung Galaxy S-6 to search for and share child pornography, and that he had been viewing child pornography just prior to accompanying the Cherokee County Sheriff's Office investigators to the 2499 Ebenezer Road residence. **HONEA** provided the unlock code to the Samsung Galaxy S-6 and signed a permission to search the Samsung Galaxy S-6. Additionally, **HONEA** gave the unlock code and permission to search another phone belonging to him, a Samsung S327VL Galaxy J3 Luna Pro.

31. At the end of the February 7, 2019, interview, **HONEA** accompanied investigators with the Cherokee County Sheriff's Office to 531 Pet Lane Road, Murphy, North Carolina and identified it as his residence. The residence is a brown wood construction house with a green roof which sits adjacent to a barn type residence. The barn type residence is the home of his landlords, Jill and Earl Ruoss. It was also the source of his internet connection. **HONEA** then gave consent for investigators to search and seize computers,

storage devices, and other electronic devices they might find from his residence at 531 Pet Lane Road. This search resulted in the seizure of the previously described Samsung Galaxy J3 phone.

32. The search of the residence at 2499 Ebenezer Road, Murphy, North Carolina resulted in the seizure of a desktop computer. As previously described, the Samsung S6 cellphone was located on **HONEA's** person. An HSI forensic analyst conducted a forensic examination on the items. 172 child pornography files were found on the computer, with six depicting children engaging in sexual acts. In the Samsung J3 Luna Pro smartphone, the examiner found 11 child pornography images.

33. In December 2019, I was given a report pertaining to a referral made by Kik that Kik user "gravity 690" had been trading child pornography. The report concerned IP address 50.111.79.154 and listed one image of child pornography that had been sent or received by the suspect user. Accompanying the report was information that the IP address that was used by Kik user "gravity 690" to upload the image of child pornography was used on April 1, 2019 at 11:25:27 UTC.

34. I have viewed the image reported by Kik and it is described as follows:

FILE: Image-gravity690_mrk-UPLOADIP-50.111.79.154-UPLOADTIME-2019-04-01-1554117927344.UTC: This image is a digital image of two prepubescent females making a lewd and lascivious display of their genitalia.

35. Provided along with the aforementioned Kik Report is a Kik subscriber record for user "gravity690." This subscriber record reveals a "registration timestamp" for user "gravity690" of March 31, 2019 at 08:56:47 UTC. The user provided his first name as "gravity" and his last name as "two." The Kik records list the email for user "gravity690" as twogravity06@gmail.com. The user's device is identified as a Samsung Android (model number: SM-S367VL). The subscriber records also indicate that the user provided that his birthdate is December 29, 1986. The subscriber records also indicate that the user "gravity690" accessed the Kik account 49 times during the period of March 31, 2019 08:56:47 UTC and April 1, 2019 10:39:07 UTC using IP address 50.111.79.154.

36. I know from previous encounters with HONEA and from records maintained at the Cherokee County Sheriff's Office that his date of birth is December 29, 1986. Thus, HONEA's date of birth is the same as what the user provided to establish the Kik account "gravity690".

37. Also provided with the information in the Kik report was a Department of Homeland Security Summons dated September 26, 2019, requesting information pertaining to IP address 50.111.79.154 during the period of April 01, 2019 11:25:27 UTC. The legal summons was directed to Frontier Communications, an internet service provider.

38. The Kik report also included a reply from Frontier Communications with the following information for the account subscriber information associated with IP address 50.111.79.154. The IP address had been assigned to the account of Earl and Jill Ruoss at 531 Pet Lane Road, Murphy, North Carolina. The IP address 50.111.79.154 had been assigned to the account of Earl and Jill Ruoss at 531 Pet Lane Road, Murphy North Carolina from a period of March 28, 2019 18:03:07 UTC to April 3, 2019 02:40:35 UTC. This time frame encompasses the entire time that the "gravity690" Kik account was established and transmitted the child pornography file Image-gravity690_mrk-UPLOADIP-50.111.79.154-UPLOADTIME-2019-04-01-1554117927344.UTC.

39. Thus, my investigation leads me to believe that the individual who uses the Kik user name "childpussy1" described in paragraphs 11 through 17 of this affidavit is in fact **BRYCE HONEA**, the same individual I have been investigating over an extended period of time.

40. On May 21, 2020, Special Agent Walton, HSI, and I made contact with Jill Ruoss to ascertain if Bryce Honea still lived at 531 Pet Lane Road. Jill Ruoss confirmed that **BRYCE HONEA** still lives in the house at 531 Pet Lane Road which law enforcement previously searched on February 7, 2019. Jill Ruoss stated that she lives in the large barn style building which is adjacent to the house that **BRYCE HONEA** is currently living in. Jill Ruoss stated that **BRYCE HONEA** has told her that the reason law enforcement had spoken with him back in February of 2019 was that he had either looked at and sent some pictures of females over the internet that did not appear to be of legal age, but that was a mistake as the images were actually of legal age females who looked younger.

41. On May 21, 2020, while speaking with Jill Ruoss, law enforcement observed that a strong secure wifi connection is available in the vicinity of 531 Pet Lane Road. Jill Ruoss identified the secure wifi connection Frontier0AA8 as the secure wifi connection to her Frontier Communications account. Jill Ruoss stated that the wifi connection Frontier0AA8 is password protected and that she has given **BRYCE HONEA** the password and allows him to use her Frontier Communications account to connect to the internet.

## BACKGROUND ON CHILD PORNOGRAPHY, COMPUTERS, AND THE INTERNET

42. I have had both training and experience in the investigation of computer-related crimes. Based on my training, experience, and knowledge, I know the following:

a. Computers and digital technology are the primary way in which individuals interested in child pornography interact with each other. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

b. Digital cameras and computers with cameras save photographs or videos as a digital file that can be directly transferred to a computer by connecting the camera or smartphone to the computer, using a cable or via wireless connections such as "WiFi" or "Bluetooth." Photos and videos taken on a digital camera or smartphone may be stored on a removable memory card in the camera or smartphone. These memory cards are often large enough to store thousands of high-resolution photographs or videos.

c. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Mobile devices such as smartphones and tablet computers

may also connect to other computers via wireless connections. Electronic contact can be made to literally millions of computers around the world. Child pornography can therefore be easily, inexpensively and anonymously (through electronic communications) produced, distributed, and received by anyone with access to a computer or smartphone.

d. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. Electronic storage media of various types - to include computer hard drives, external hard drives, CDs, DVDs, and "thumb," "jump," or "flash" drives, which are very small devices that are plugged into a port on the computer - can store thousands of images or videos at very high resolution. It is extremely easy for an individual to take a photo or a video with a digital camera or camera-bearing smartphone, upload that photo or video to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices. Some media storage devices can easily be concealed and carried on an individual's person. Smartphones and/or mobile phones are also often carried on an individual's person.

e. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

f. Individuals also use online resources to retrieve and store child pornography. Some online services allow a user to set up an account with a remote computing service that may provide email services and/or electronic storage of computer files in any variety of formats. A user can set up an online storage account (sometimes referred to as "cloud" storage) from any computer or smartphone with access to the Internet. Such an account can also be accessed in the same way. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer, smartphone, or external media in most cases.

g. A growing phenomenon related to smartphones and other mobile computing devices is the use of mobile applications, also referred to as "apps." Apps consist of software downloaded onto mobile devices that enable users to perform a variety of tasks – such as engaging in online chat, sharing digital files, reading a book, or playing a game – on a mobile device. Individuals commonly use such apps to receive, store, distribute, and advertise child pornography, to interact directly with

other like-minded offenders or with potential minor victims, and to access cloud-storage services where child pornography may be stored

h. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional (*i.e.*, by saving an email as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files) or unintentional. Digital information, such as the traces of the path of an electronic communication, may also be automatically stored in many places (*e.g.*, temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

i. Individuals involved in the receipt, possession, and/or distribution of child pornography very frequently possess multiple devices that contain evidence of their interaction with child pornography and/or sexual interest in minors. In modern American culture, most individuals possess multiple devices that have the ability to connect to the Internet (e.g., tablets, desktop computers, laptop computers, and

mobile phones). Many individuals also keep prior versions of their devices (e.g., prior cell phones and prior computers). This is the case because (1) individuals are often reluctant to discard devices that frequently contain significant personal information and (2) current devices may malfunction and prior versions can often be used until the current device is repaired or replaced.

## SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

43. As described above and in Attachment B, this application seeks permission to search for records that might be found at the SUBJECT PREMISES, in whatever form they are found. One form in which the records are likely to be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

44. I submit that if a computer or storage medium is found at the SUBJECT PREMISES, there is probable cause to believe those records referenced above will be stored on that computer or storage medium, for at least the following reasons:

a. Deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

b. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts

from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

45. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium at the SUBJECT PREMISES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, email programs, and

chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. Information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (*e.g.*, registry information, communications, images and movies, transactional information, records of session times and durations, Internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a

residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, computers typically contain information that logs: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the Internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media

(*e.g.*, a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (*e.g.*, Internet searches indicating criminal planning), or consciousness of guilt (*e.g.*, running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a

review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

f. I know that when an individual uses a computer to obtain or access child pornography, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received;

notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

46. Based upon my training and experience and information relayed to me by agents and others involved in the forensic examination of computers, I know that computer data can be stored on a variety of systems and storage devices, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact disks, magnetic tapes, memory cards, memory chips, and online or offsite storage servers maintained by corporations, including but not limited to "cloud" storage. I also know that during the search of the premises it is not always possible to search computer equipment and storage devices for data for a number of reasons, including the following:

a. Searching computer systems is a highly technical process that requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is impossible to bring to the search site all of the technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may also be necessary to consult with computer personnel

who have specific expertise in the type of computer, software, or operating system that is being searched;

b. Searching computer systems requires the use of precise, scientific procedures which are designed to maintain the integrity of the evidence and to recover "hidden," erased, compressed, encrypted, or password-protected data. Computer hardware and storage devices may contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Since computer data is particularly vulnerable to inadvertent or intentional modification or destruction, a controlled environment, such as a law enforcement laboratory, is essential to conducting a complete and accurate analysis of the equipment and storage devices from which the data will be extracted.

c. The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the premises; and

d. Computer users can attempt to conceal data within computer equipment and storage devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files;

however, a user can easily change the extension to ".txt" to conceal the image and make it appear that the file contains text. Computer users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. In addition, computer users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography a computer user can conceal text in an image file which cannot be viewed when the image file is opened. Therefore, a substantial amount of time is necessary to extract and sort through data that is concealed or encrypted to determine whether it is contraband, evidence, fruits, or instrumentalities of a crime.

47. Additionally, based upon my training and experience and information relayed to me by agents and others involved in the forensic examination of computers, I know that routers, modems, and network equipment used to connect computers to the Internet often provide valuable evidence of, and are instrumentalities of, a crime. This is equally true of wireless routers, which create localized networks that allow individuals to connect to the Internet wirelessly. Though wireless networks may be secured (in that they require an individual to enter an alphanumeric key or password

before gaining access to the network) or unsecured (in that an individual may access the wireless network without a key or password), wireless routers for both secured and unsecured wireless networks may yield significant evidence of, or serve as instrumentalities of, a crime—including, for example, serving as the instrument through which the perpetrator of the Internet-based crime connected to the Internet and, potentially, containing logging information regarding the time and date of a perpetrator's network activity as well as identifying information for the specific device(s) the perpetrator used to access the network. Moreover, I know that individuals who have set up either a secured or unsecured wireless network in their residence are often among the primary users of that wireless network.

48. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

**AUTHORITY TO COMPEL BRYCE HONEA TO UNLOCK HIS MOBILE DEVICE WITH HIS FINGERPRINT OR FACIAL RECOGNITION**

49. Based on information provided by Kik Interactive and my prior encounters with **BRYCE HONEA**, **BRYCE HONEA** is believed to be in possession of a mobile electronic cellular device. This device may offers its user the ability to unlock the device via the use of a fingerprint or thumbprint (collectively, "fingerprint") in lieu of a numeric or alphanumeric passcode or password. This feature is generically referred to as a "fingerprint sensor." Alternatively, it may offer its user the ability to unlock the device via facial recognition.

50. If a user enables the fingerprint sensor, he or she can register up to various fingerprints that can be used to unlock that device. The user can then use any of the registered fingerprints to unlock the device by pressing the relevant finger(s) to the device's fingerprint sensor, which is found below the display found at the bottom of the front of the device. In my training and experience, users of mobile devices that offer fingerprint sensor or Touch IDs (Apple iOS devices) often enable it because it is considered to be a more convenient way to unlock the device than by entering a numeric or alphanumeric passcode or password, as well as a more secure way to protect the device's contents. This is particularly true when the user(s) of the device

are engaged in criminal activities and thus have a heightened concern about securing the contents of the device.

51. In some circumstances, a fingerprint cannot be used to unlock a device that has fingerprint sensor enabled, and a passcode or password must be used instead. These circumstances include: (1) when more than 72 hours have passed since you unlocked the phone. Thus, in the event law enforcement encounters a locked device, the opportunity to unlock the device via fingerprint sensor exists only for a short time. The fingerprint sensor also will not work to unlock the device if (1) the device has been turned off or restarted; and (2) some number, (often five) unsuccessful attempts to unlock the device via Fingerprint Sensor are made.

52. The passcode or password that would unlock a mobile device in **HONEA's** possession is not known to law enforcement. Thus, it may be necessary to press the finger(s) of **HONEA** to the device's fingerprint sensor in an attempt to unlock the device for the purpose of executing the search authorized by this warrant. Attempting to unlock the relevant device(s) via fingerprint sensor with the use of the fingerprints of the user(s) is necessary because the government may not otherwise be able to access the data contained on those devices for the purpose of executing the search authorized by this warrant. It may also be necessary to hold the device in front of **HONEA's** face

in order to activate the facial recognition unlock feature.

53. Based on these facts as stated in the affidavit, and my training and experience, it is likely that **HONEA** is the only user of the mobile device in his possession and thus that his fingerprints or facial features are among those that are able to unlock the device.

54. Although it is not known which of a given user's 10 fingerprints is capable of unlocking a particular device, based on my training and experience I know that it is common for a user to unlock a fingerprint sensor enabled device via the fingerprints on thumbs or index fingers. In the event that law enforcement is unable to unlock the mobile device as described above within the attempts permitted by the fingerprint sensor, this will simply result in the device requiring the entry of a password or passcode before it can be unlocked.

55. Due to the foregoing, I request that the Court authorize law enforcement to press the fingers (including thumbs) of **HONEA** to the fingerprint sensor of the subject mobile device for the purpose of attempting to unlock the device via the fingerprint sensor in order to search the contents as authorized by this warrant. Alternatively, I request that the Court authorize law enforcement to hold the device in front of **HONEA's** face in order to activate the facial recognition feature.

## CONCLUSION

56. Based on the foregoing, there is probable cause to believe that the federal criminal statutes cited herein have been violated, and that the contraband, property, evidence, fruits and instrumentalities of these offenses, more fully described in Attachment B, are located at the location described in Attachment A. I respectfully request that this Court issue a search warrant for the location described in Attachment A, authorizing the seizure and search of the items described in Attachment B.

***REVIEWED BY ASSISTANT UNITED STATES ATTORNEY***

***DAVID A. THORNELOE***

***This, the 26th Day of May 2020.***

_/R.L. Williams/_____
R. L. Williams
Task Force Officer
Homeland Security Investigations

In accordance with Rule 4.1(b)(2)(A), the Affiant attested under oath to the contents of this Affidavit, which was submitted to me by reliable electronic means, on this 27th day of May, 2020, at 9:18 AM

Signed: May 27, 2020

W. Carleton Metcalf
United States Magistrate Judge

## DESCRIPTION OF LOCATION TO BE SEARCHED

The property to be searched is 531 Pet Lane Road, Murphy, North Carolina 28906, to include any outbuildings and vehicles associated with the premises or people at the premises, but not to include the adjacent barn-style structure. If located thereon, law enforcement may search any computer devices (including cellular telephones, smart phones, or mobile devices) located on any person located therein.

The premises of 531 Pet Lane Road, Murphy, North Carolina 28906, is further described as a single one and a half story residence, with a green roof. The residence is located at the end of Pet Lane Road and adjacent to a larger barn-style structure. Pet Lane Road has a road sign prominently displayed at the entrance of Dockery Creek Road, Murphy North Carolina. Pet Lane Road is first road that runs to the right off Dockery Creek Road once you turn right from Ebenezer Road.

## ATTACHMENT B

## ITEMS TO BE SEIZED

The following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely violations of Title 18, United States Code, Sections 2252 and 2252A:

1. Computers or storage media used as a means to commit the violations described above.
2. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):
    a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to the crime(s) under investigation and to the computer user;

e. evidence indicating the computer user's knowledge and/or intent as it relates to the crime(s) under investigation;

f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

g. evidence of programs (and associated data) that are designed to eliminate data from the COMPUTER;

h. evidence of the times the COMPUTER was used;

i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

k. records of or information about Internet Protocol addresses used by the COMPUTER;

l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and

m. contextual information necessary to understand the evidence described in this attachment.

3. Routers, modems, and network equipment used to connect computers to the Internet.

4. Child pornography and child erotica.

5. Records, information, and items relating to violations of the statutes described above including:

a. Records, information, and items relating to the occupancy or ownership of the SUBJECT PREMISES, including utility and telephone bills, mail envelopes, or addressed correspondence;

b. Records, information, and items relating to the ownership or use of computer equipment found in the above residence, including sales receipts, bills for Internet access, and handwritten notes;

c. Records and information relating to the identity or location of the persons suspected of violating the statutes described above;

d. Records and information relating to the sexual exploitation of children, including correspondence and communications.

e. Records and information relating or pertaining to the identity of the person or persons using or associated with the internet provider.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers,

notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact discs, magnetic tapes, memory cards, memory chips, and other magnetic or optical media.

This warrant authorizes law enforcement to compel the owner of a mobile device (such as a smart phone, cellular device, tablet computer) subject to this warrant to unlock the device using a fingerprint, thumbprint, or facial recognition.